



ВЫБОР ВАРИАНТА СИСТЕМЫ ЗАЩИТЫ ЦЕНТРОВ ОБРАБОТКИ ДАННЫХ

В.В. Павельев, С.В. Павельев

Предложена модель выбора варианта защиты выделенного центра обработки данных от аварий и катастроф в территориально-распределенной автоматизированной системе, построенной с использованием каналов глобальных сетей связи. В модели применен метод векторной стратификации многомерных объектов и методы анализа и управления рисками.

Ключевые слова: выбор вариантов, защита от аварий и катастроф, обработка данных, метод векторной стратификации, многомерный объект.

ВВЕДЕНИЕ

Многие организации целенаправленно внедряют технологии обеспечения непрерывности и безопасности бизнеса в непредвиденных ситуациях. Поскольку затраты на внедрение и эксплуатацию таких технологий составляют значительную долю ресурсов многих организаций, важное значение приобретает проблема оптимизации этих затрат. Один из основных подходов, применяемых в настоящее время для оптимизации затрат на системы безопасности, состоит в анализе и управлении рисками [1–4]. В качестве меры риска используется пара показателей: определяемые экспертами мера возможности неблагоприятного события Q и последствия (ущерб) W при его наступлении. Оба показателя могут быть мультипликативным образом объединены в один: $R = QW$, что позволяет сравнивать ситуации с различными последствиями и возможностями их наступления [1].

Развитие информационных технологий позволило строить автоматизированные системы управления бизнес-процессами, распределенными на значительной территории (например, управление работой транснациональных корпораций). При этом необходимая информация сосредоточивается в Центрах обработки данных (ЦОД), обеспечивающих ее своевременное обновление и разрешенный доступ для клиентов.

Принятие ответственных решений по выбору схемы защиты ЦОД от аварий и катастроф в процессе проектировании территориально-распределенной автоматизированной системы требует всесторонней комплексной оценки рассматриваемых

вариантов, механизм которой прозрачен и понятен для лиц, принимающих решения. В качестве основных частных критериев учитываются следующие показатели:

- возможный ущерб от нарушения нормальной работы автоматизированной системы в результате выхода из строя ЦОД;
- мера возможности наступления событий, наносящих существенный ущерб;
- затраты (капитальные и эксплуатационные) на мероприятия по защите ЦОД от аварий и катастроф.

В связи с этим, актуально решение задачи комплексной оценки и обоснованного выбора лучшего варианта системы защиты ЦОД из множества возможных альтернативных решений.

1. ОБЕСПЕЧЕНИЕ ТРЕБУЕМОГО УРОВНЯ ДОСТУПНОСТИ ИНФОРМАЦИОННЫХ РЕСУРСОВ В ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЕННЫХ АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

При эксплуатации любых автоматизированных систем всегда существует определенная возможность разрушения информационных массивов (ИМ) и программных модулей (ПМ). Для обеспечения сохранности информации и повышения живучести системы обычно применяют методы резервирования — создается резерв из некоторого числа копий и (или) предысторий ИМ и ПМ, предусматривается также резервирование средств обработки данных и каналов связи. Каналы глобальных сетей связи позволяют территориально разнести узлы с резервом ИМ и ПМ, что существенно

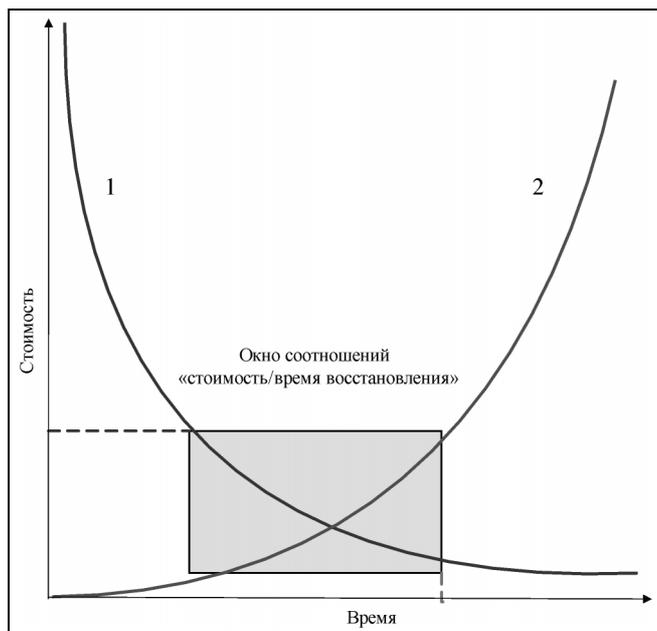


Рис. 1. Зависимости финансовых потерь (2) из-за недоступности информационных ресурсов от времени их недоступности и стоимости (1) создания системы высокой доступности от допустимого времени простоя

повышает возможность сохранения доступности данных при различных авариях и катастрофических ситуациях (пожары, землетрясения, наводнения и др.), в случае возникновения которых могут быть уничтожены (или выведены из строя на длительный срок) все локально расположенные копии ИМ и ПМ (как основные, так и резервные) и (или) элементы поддерживающей инфраструктуры. При использовании каналов глобальных сетей связи и децентрализованном хранении резерва возможно быстрое возобновление работы при выходе из строя одного из узлов, содержащего рабочие информационные массивы и программные модули, и (или) обслуживающих его каналов связи. Зависимость финансовых потерь, которые несет организация из-за недоступности ИТ-сервисов (служб и средств, поддерживающих информационные технологии (ИТ), необходимые для реализации бизнес-процесса) от времени их недоступности, приведена на рис. 1. Здесь же приведена зависимость стоимости создания системы высокой доступности от допустимого времени простоя. Размер финансовых потерь, как правило, растет нелинейно, нелинейная зависимость наблюдается и у размера затрат на мероприятия по обеспечению непрерывности ИТ-сервисов от гарантированного времени восстановления. Оптимальное решение обычно лежит в области, которая на рисунке обозначена как окно соотношений «стоимость/время восстановления» [5].

2. ОСНОВНЫЕ СХЕМЫ ОРГАНИЗАЦИИ РЕЗЕРВИРОВАНИЯ ИНФОРМАЦИОННЫХ МАССИВОВ И ИТ-СЕРВИСОВ В ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЕННЫХ СИСТЕМАХ

Архитектура современных территориально-распределенных автоматизированных систем обычно предусматривает один или несколько ЦОД, иногда находящихся на значительном расстоянии друг от друга. Приняв за основу семиуровневую классификацию построения систем резервирования и управления данными [5] и опираясь на отечественный и международный опыт построения территориально-распределенных ИТ-архитектур с выделенными ЦОД [6—8], авторы определили 10 следующих наиболее распространенных схем (уровней) организации резервирования информационных массивов и ИТ-сервисов в системах данного класса.

- Регулярное резервное копирование ИМ и ПМ с хранением резервных копий в том же помещении (здании).
- Регулярное резервное копирование с хранением резервных копий в отдельном помещении (здании). Данные на извлекаемых носителях регулярно вывозятся на хранение в отдельное защищенное помещение (здание).
- Применяются технологии резервного копирования и архивирования данных на резервную площадку. Дополнительно, в законсервированном состоянии, существует резервный центр.
- Применяются технологии резервного копирования и архивирования наиболее критичных данных на резервную площадку по каналам связи. Резервный центр не законсервирован полностью, а осуществляет по сети регулярное копирование наиболее часто обновляемых и самых критичных для бизнеса данных.
- Репликация данных на резервную площадку в асинхронном режиме (с небольшим запаздыванием).
- Репликация данных на резервную площадку в синхронном режиме.
- Оперативное резервирование. Режим постоянной готовности. Репликация данных на резервную площадку осуществляется в синхронном режиме.
- Вычислительный центр распределен по нескольким площадкам, находящимся на удалении не более 50 км. В этом случае из нескольких площадок можно создать единый вычислительный центр, рассматривая их просто как разные комнаты в одном здании.
- Вычислительный центр распределен по нескольким площадкам, находящимся на существенном удалении (в несколько тысяч километров).
- Вычислительный центр состоит из нескольких площадок, расположенных в пределах одного го-



рода, плюс одна или несколько площадок на существенном удалении (в другом регионе). Между площадками в пределах города организована синхронная репликация, на удаленные площадки осуществляется асинхронная репликация.

3. МОДЕЛЬ КОМПЛЕКСНОЙ ОЦЕНКИ И ВЫБОРА ВАРИАНТА ЗАЩИТЫ ЦЕНТРА ОБРАБОТКИ ДАННЫХ ОТ АВАРИЙ И КАТАСТРОФ

Широко распространены методики выбора лучших вариантов, в которых в качестве целевой функции принята аддитивная линейная свертка частных показателей с весовыми коэффициентами. В частности, такая свертка применяется в качестве целевой функции в известном методе анализа иерархий Т. Саати. Она предполагает инвариантность весового коэффициента каждого из частных показателей относительно изменений фиксированных значений остальных показателей, а также допустимость взаимной компенсации худших оценок по одним показателям лучшими оценками по другим показателям, что на практике далеко не всегда выполняется. Модель $M = \langle A, S, F \rangle$ решения задачи целенаправленного выбора лучшего варианта на основе метода векторной стратификации [9] свободна от перечисленных недостатков. Здесь A — заданная формулировка цели, S — структура критериально-целевых свойств (показателей) оцениваемых объектов, F — решающее правило, функция выбора, комплексный критерий.

Особенности модели:

- в явном виде используется заданная документированная формулировка цели, отсутствующая в типичных моделях принятия решений, где это приводит к неопределенности в выборе системы показателей;

- путем дихотомической декомпозиции заданной формулировки цели строится древовидная структура показателей комплексной оценки (бинарная иерархия подцелей, а также характеристик и параметров средств, необходимых для их достижения, совокупность значений которых определяет степень достижения заданной цели);

- в узловых вершинах полученной древовидной структуры показателей размещаются «матрицы последовательной логической свертки» оценок по показателям нижнего уровня иерархии в комплексную оценку, в совокупности образующие решающее правило, комплексный критерий;

- имеется возможность не только выбрать лучший вариант из рассматриваемых, но и оптимизировать сочетание его параметров по комплексному критерию.

- значения показателей могут быть представлены как в числовом, так и в словесном выраже-

нии, например, оценка — очень высокая, высокая, средняя, низкая, очень низкая.

Оценка соответствия фактического значения P_i рассматриваемого показателя предъявляемым требованиям производится следующим образом (применяются два варианта оценки).

Вариант 1. Оценка Y фактического значения показателя P_i , измеренного в числовой шкале, вычисляется по формуле: $Y = (P_i - P_{\min}) / (P_{\max} - P_{\min})$, если P_{\max} — требуемое для полного достижения заданной цели идеальное значение измеряемого показателя, а P_{\min} — наибольшее из практически бесполезных для достижения заданной цели значение измеряемого показателя. Если наилучшим является наименьшее значение показателя, то оценка фактического значения показателя P_i определяется по формуле $Y = (1/P_i - 1/P_{\max}) / (1/P_{\min} - 1/P_{\max})$, где P_{\min} — идеальное значение измеряемого показателя, а P_{\max} — наименьшее из практически бесполезных для достижения заданной цели значение измеряемого показателя.

Далее с помощью вербально-числовой психофизической шкалы Харрингтона [10] формируется шкала стратификации и соответствующая ей балльная шкала:

- 5-я страта: $0,8 < Y \leq 1 \Rightarrow 5$ баллов;
- 4-я страта: $0,63 < Y \leq 0,8 \Rightarrow 4$ балла;
- 3-я страта: $0,37 < Y \leq 0,63 \Rightarrow 3$ балла;
- 2-я страта: $0,2 < Y \leq 0,37 \Rightarrow 2$ балла;
- 1-я страта: $0 < Y \leq 0,2 \Rightarrow 1$ балл.

Вариант 2. Экспертная оценка Y фактического значения показателя P_i , включая нечисловое, определяется как соответствующая точка на балльной шкале, задаваемой следующими реперными точками на интервале $P_{\max} - P_{\min}$:

$Y = 5$ баллов $\Rightarrow P_i = P_{\max}$ (или P_{\min} , в зависимости от смысла показателя) — требуемое для полного достижения заданной цели идеальное значение показателя,

$Y = 4$ балла $\Rightarrow P_i = P_4$ (хорошее значение);

$Y = 3$ балла $\Rightarrow P_i = P_3$ (удовлетворительное значение);

$Y = 2$ балла $\Rightarrow P_i = P_2$ (плохое значение);

$Y = 1$ балл $\Rightarrow P_i = P_{\min}$ (или P_{\max} , в зависимости от смысла показателя) — бесполезное для достижения заданной цели значение показателя.

Между реперными точками находятся страты с дробными значениями баллов:

5-я страта: $4 \text{ баллов} < Y < 5 \text{ баллов}$;

4-я страта: $3 \text{ баллов} < Y < 4 \text{ баллов}$;

3-я страта: $2 \text{ баллов} < Y < 3 \text{ баллов}$;

2-я страта: $1 \text{ баллов} < Y < 2 \text{ баллов}$;

1-я страта: $Y \leq 1$ балла.

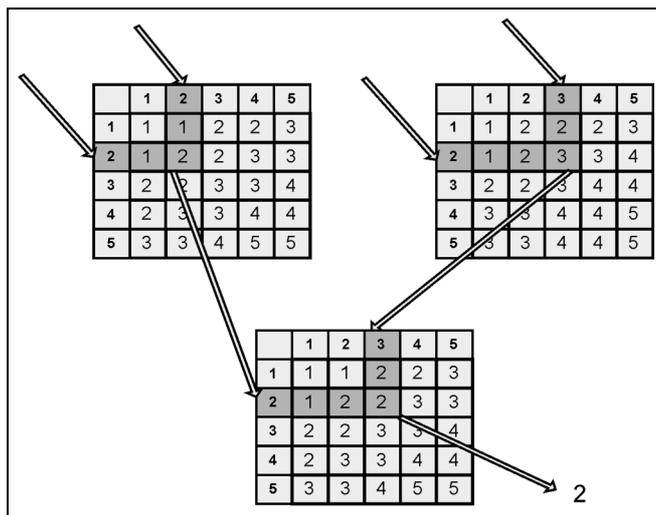


Рис. 2. Фрагмент решающего правила комплексной оценки

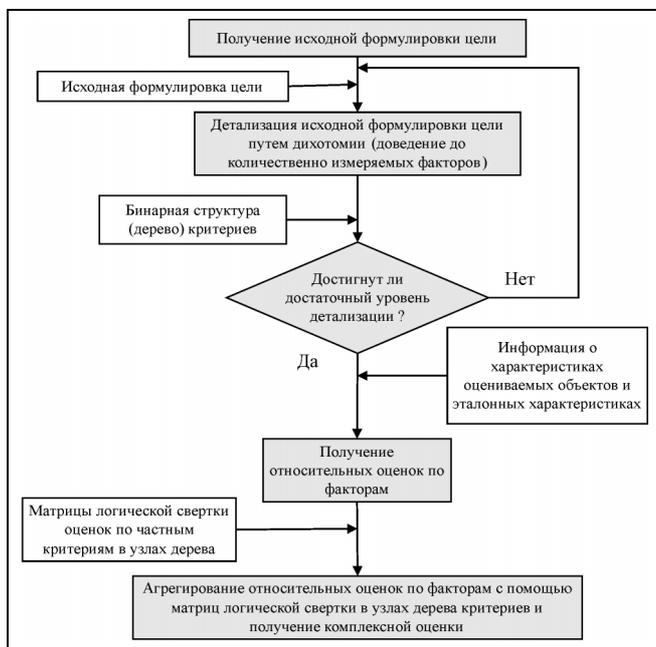


Рис. 3. Алгоритм комплексной оценки

По реперным точкам путем интерполяции строятся непрерывные функции $Y = f(P)$.

Для каждого узла древовидной структуры показателей лицо, принимающее решение, или эксперты заполняют матрицы размерности 5×5 логической свертки частных оценок в баллах в обобщающую оценку. Строки матрицы соответствуют значениям оценок по одному из объединяемых показателей, столбцы — значениям оценок по второму показателю. Значения оценок варианта по обобщающему показателю проставляются на пере-

сечении столбцов и строк. Их определяет эксперт или лицо, принимающее решение, с учетом относительной значимости оценок по объединяемым показателям.

Заполненные матрицы логической свертки показателей, помещенные в соответствующих узлах древовидной структуры комплексного критерия, порождают решающее правило комплексной оценки. Оно может быть реализовано в виде компьютерной программы. Пример фрагмента такого правила представлен на рис. 2.

С помощью этого решающего правила все оцениваемые объекты можно разделить на 5 страт, упорядоченных по их предпочтительности. Самые лучшие отнесены к 5-й страте, самые худшие — к 1-й.

Алгоритм комплексной оценки представлен на рис. 3.

Рассмотрим решение задачи выбора лучшей схемы защиты ЦОД из десяти приведенных в § 2 наиболее распространенных и обеспеченных современными программными и техническими средствами схем.

Основные процедуры процесса комплексного оценивания и выбора лучшего варианта защиты состоят в следующем.

1. Формулировка цели: обеспечение минимального риска нарушения доступности информационных ресурсов ЦОД при приемлемой стоимости создания и эксплуатации системы защиты центра от аварий и катастроф.

2. С помощью регулярной процедуры путем дихотомии, формируется древовидная структура по-

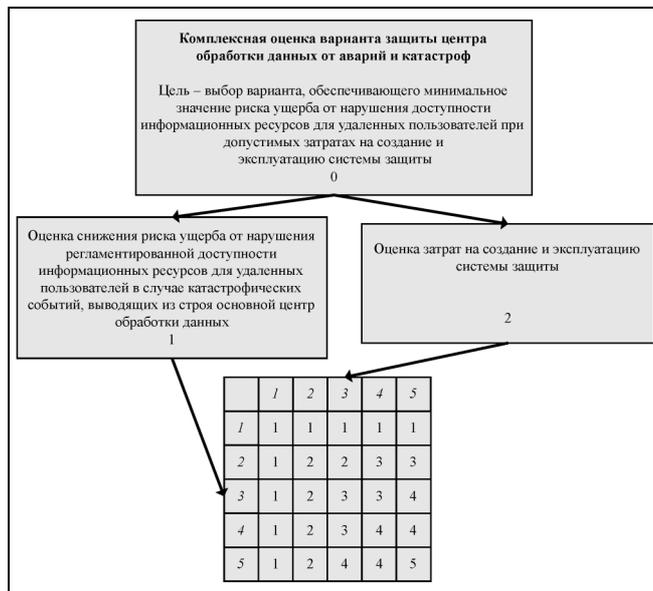


Рис. 4. Фрагмент древовидной структуры показателей комплексного критерия



Фрагменты показателей групп П1 и П2

Код показателя	Наименование показателя
<i>Группа П1</i>	
1.1.1.1.2	Оценка снижения риска ущерба от недоступности средств обработки данных вследствие природных пожаров, наводнений и прочих негативных природных факторов
1.1.1.2.1.1	Оценка снижения риска ущерба от недоступности средств обработки данных вследствие аварий на опасных производствах
1.1.1.2.1.2	Оценка снижения риска ущерба от недоступности средств обработки данных вследствие прочих негативных техногенных воздействий
<i>Группа П2</i>	
2.1.1.1	Оценка затрат на закупку оборудования и организацию каналов связи производственной площадки
2.1.1.2	Оценка затрат на закупку оборудования и организацию каналов связи резервной площадки
2.1.2.1	Оценка затрат на оборудование помещений производственной площадки
2.1.2.2	Оценка затрат на оборудование помещений резервной площадки
2.2.1.1	Оценка текущих затрат на эксплуатацию системы, находящейся в производственном режиме
2.2.1.2	Оценка текущих затрат на эксплуатацию системы, находящейся в резерве
2.2.2	Оценка затрат на оплату труда персонала

казателей комплексного критерия, отражающая их причинно-следственную связь с формулировкой цели. Ограниченный объем статьи не позволяет привести структуру и состав показателей полностью. Фрагмент прикорневой части этой структуры представлен на рис. 4.

3. Выделение групп конечных показателей: группа П1 — показатели, определяющие снижение риска ущерба благодаря мерам защиты; группа П2 — показатели, определяющие размер затрат на создание системы защиты.

В таблице в качестве примера приведена часть показателей групп П1 и П2.

4. Определение путем опроса экспертов меры возможности реализации отдельных опасностей (находящихся на нижних ветвях дерева опасностей) в отношении выделенных групп объектов опасности в случае отсутствия мероприятий по защите ЦОД от аварий и катастроф.

5. Расчет ущерба в случае реализации опасностей (находящихся на нижних ветвях дерева опас-

ностей) при отсутствии мероприятий по защите ЦОД от аварий и катастроф.

6. Расчет суммарного риска нарушения доступности информационных ресурсов при отсутствии мероприятий по защите ЦОД от аварий и катастроф: $R_{\Sigma} = \sum_i Q_i W_i$, где Q_i и W_i — определяемая эк-

спертами мера возможности реализации опасностей и ущерб в случае их реализации в отношении i -й группы объектов опасности. Каждой группе объектов опасности соответствует риск $R_i = Q_i W_i$.

7. Расчет затрат на реализацию каждого варианта для имеющегося перечня вариантов защитных мероприятий: $C_n = \sum_i C_{ni}$, где n — номер рассматриваемого варианта, i — статья затрат в соответствии с деревом затрат.

8. Исключение из перечня рассматриваемых вариантов всех вариантов, не соответствующих условию

$$C_n \leq kR_{\Sigma}, \quad (1)$$

где R_{Σ} — суммарный риск нарушения доступности информационных ресурсов при отсутствии мероприятий по защите ЦОД от аварий и катастроф, k — коэффициент, отражающий склонность лица, принимающего решения к риску.

9. Расчет значений рисков для каждой группы объектов опасности для каждого из рассматриваемых вариантов после исключения вариантов, не соответствующих условию (1): $R_{ni} = Q_{ni} W_{ni}$, где n — номер варианта; i — номер группы опасностей, воздействующих на определенную группу объектов опасностей. Например, $R_{n1.1.1.1.1} = Q_{n1.1.1.1.1} W_{n1.1.1.1.1}$ — риск ущерба от недоступности средств обработки данных по причине неработоспособности основного производственного оборудования или персонала вследствие ураганов и землетрясений.

10. Расчет размера снижения риска — для каждого из рассматриваемых вариантов вычисляются размеры снижения риска для каждой группы объектов опасности по сравнению с размерами рисков, рассчитанными для случая отсутствия мер защиты (см. п. 6) по формуле $\Delta R_{ni} = R_i - R_{ni}$.

11. Получение оценок по показателям — размеры величин снижения риска и постатейных расходов на создание систем защиты, характеризующих каждый из рассматриваемых вариантов, преобразуются в единую шкалу из пяти градаций.

12. Заполнение матриц логической свертки частных оценок в обобщающую оценку.

13. Оценка по комплексному критерию и выбор лучшего варианта защиты.

ЗАКЛЮЧЕНИЕ

Рассмотрены основные стратегии обеспечения доступности информационных ресурсов и обеспечения непрерывности IT-сервисов в случае аварий и катастроф. На основе анализа российского и международного опыта построения территориально-распределенных IT-архитектур выделены 10 наиболее распространенных схем (уровней) защиты центров обработки данных, обеспеченных современными программно-техническими средствами. Разработана модель выбора лучшего варианта системы защиты ЦОД, позволяющая учитывать специфику конкретной организации в части соотношения ценности используемой информации и затрат на создание системы ее защиты. Используются как количественные (числовые), так и качественные (вербальные) исходные данные. Применение в модели матриц логической свертки оценок по частным критериям в обобщающую оценку обеспечивает прозрачность и наглядность решающего правила выбора для лиц, принимающих решения.

ЛИТЕРАТУРА

1. Вишняков Я.Д., Радаев Н.Н. Общая теория рисков. — М.: Изд. центр «Академия», 2007. — 390 с.
2. Соложенцев Е.Д. Сценарное логико-вероятностное управление риском в бизнесе и технике. — СПб.: Изд. дом «Бизнес-пресса», 2004. — 176 с.
3. Управление рисками: обзор потребительных подходов. Ч. I // Jet Info. — 2006. — № 11 (162). — С. 2—15
4. Управление рисками: обзор потребительных подходов. Ч. II // Там же. — № 12 (163). — С. 2—19.
5. IBM Total Storage Business Continuity Solutions Guide/ C.Warrick ets. — International Technical Support Organization. — IBM Redbooks SG24-6547-02. — August 2005. — P. 49.
6. Голубев Д.Л. Распределенные центры обработки данных // Jet Info. — 2006. — № 5 (156). — С. 3—15.
7. Массиглиа П. Технологии управления хранением данных компании VERITAS Software // Jet Info. — 2001. — N 8 (99). — С. 3—44.
8. Гончаров А. Методы защиты данных: обзор решений // Storage News — 2006. — № 2 (27). — С. 20—23.
9. Готов В. А., Павельев В.В. Векторная стратификация. — М.: Наука, 1984. — 95 с.
10. Harrington E.C. The Desirability Function // Industrial Quality control. — 1965. — Vol. 21, N 10. — P. 494—498.

Статья представлена к публикации членом редколлегии В.В. Кульбой.

Павельев Владимир Васильевич — ст. науч. сотрудник, Институт проблем управления им. В.А. Трапезникова РАН, г. Москва, ☎ (495) 334-88-21, e-mail: pavvvs@ipu.ru,

Павельев Сергей Владимирович — вед. эксперт, Департамент информатизации ОАО «Федеральная сетевая компания Единой энергетической системы РФ», г. Москва, ☎ (985) 921-76-07, e-mail: paveljev-sv@rao.elektra.ru

Новая книга

Вишневский В.М., Семенова О.В. Системы поллинга: теория и применение в широкополосных беспроводных сетях. — М.: Техносфера, 2007. — 312 с.

При проектировании и оценке производительности беспроводных сетей передачи информации с централизованным управлением широко применяются модели поллинга (циклического опроса), которые активно разрабатываются и исследуются с конца 1950-х гг.

Систематизация и обобщение теоретических результатов, полученных в данной области до 1985 г., проведены в монографии Х. Такаги "Analysis of polling systems" (MIT Press, 1986). Дальнейшее развитие теоретических результатов в этом направлении, опубликованных до 1995 г., нашло отражение в монографии С. Борста "Polling systems" (Amsterdam: Stichting Mathematisch Centrum, 1996). Однако быстрое развитие телекоммуникационных систем и сетей, в частности, систем сотовой связи и широкополосных беспроводных сетей, потребовало разработки новых методов анализа и синтеза систем поллинга. Поэтому в последнее десятилетие появилось значительное число работ по системам поллинга в этом направлении.

Настоящая монография посвящена обобщению и систематизации методов исследования стохастических моделей поллинга и применения их для проектирования широкополосных беспроводных сетей Wi-Fi и Wi-MAX с централизованным механизмом управления. Рассмотрены новые модели, адекватно описывающие функционирование широкополосных беспроводных сетей под управлением протоколов IEEE 802.11 и IEEE 802.16. Даны определение и классификация систем поллинга. Изложены условия стационарности и методы анализа и оптимизации характеристик систем поллинга. Представлены системы с механизмом резервирования и пороговыми дисциплинами обслуживания, а также новые модели с ограниченным обслуживанием очередей, анализ которых представляет как теоретический, так и практический интерес. Рассмотрены приоритетные системы, представляющие собой отдельный класс системы поллинга. Приведены численные результаты проектирования и оценки производительности широкополосных беспроводных сетей с централизованным управлением и механизмом циклического опроса.

Значительный интерес представляют вошедшие в книгу оригинальные теоретические результаты авторов по адаптивному поллингу и практическое использование этих результатов в разработанном ИППИ РАН аппаратно-программном комплексе радиоэлектронной системы РАПИРА, которая в настоящее время серийно выпускается отечественной промышленностью.

Монография отражает дальнейшее развитие теоретических основ проектирования компьютерных сетей и может рассматриваться как второй том книги В.М. Вишневского "Теоретические основы проектирования компьютерных сетей" (М.: Техносфера, 2003).

Для специалистов в области стохастических систем, проектировщиков компьютерных сетей, аспирантов и студентов высших учебных заведений.